[Add school logo and name]

part of the

LDBS Academies Trust

LAT and LAT 2

ICT Acceptable Use Policy
Staff, visitors and pupils

Document type	School Policy	Statutory DfE / Trust	DfE
Approval Level	Trust Board of Directors	Review Frequency	Biennial
Approval date	21/05/2026	Next Review Date	20/05/2028
On behalf of the Trust Board of Directors			
Name	Andrew Garwood-Watkins	Name	Christalla Jamil
Position	Chair of the Board of Trustees of the Trusts	Position	CEO of the Trusts
On behalf of Choose an item.			
Name		Name	
Position	Chair of the School Board of Governors	Position	Headteacher
Publication to	☒ GovHub	☐ Staff info site	☒ Website

NOTE TO THE LOCAL ACADEMY COMMITTEES – MAY BE DELETED UPON LAC ADOPTION

This is the Trust-wide Acceptable Use (Staff and Visitors) Policy template. A space is foreseen above for the school to add its own name and logo. A box below is foreseen for the school to add its school-specific Values. Annex 1 should be completed by the school with the school-specific information. Please do not change the formatting of titles etc as the Policy contains cross-references. This document sets minimum compliance requirements for all LDBS Academies Trust (LAT and LAT 2) schools. Each Local Academy Committee (LAC) is requested to: (i) Approve this template (with Annex 1 - School-specific details) completed; (ii) Ensure local implementation complies with this template.

Version control update log: This version is entirely new on the Trust level. Care has been taken to ensure consistency and referral to existing policies, but please contact the Trust asap should you nevertheless notice any inconsistencies. PLEASE UPDATE THE TABLE OF CONTENTS FOLLOWING THE REMOVAL OF THIS SECTION (Go stand on the table of contents and you will see an "update this table" button on the top right)!

TRUST VISION STATEMENT

"The kingdom of heaven is like a mustard seed, which a man took and planted in his field. Though it is the smallest of all seeds, yet when it grows, it is the largest of garden plants and becomes a tree, so that the birds come and perch in its branches." (Matthew 13: 31-32)

In the parable of The Mustard Seed, Jesus reminds us that even the smallest of seeds has the potential to grow into the fullness of itself. We aim to provide the right environment for our children, and all whom we serve, to flourish into the fullness of themselves. He tells us these seeds grow into trees, capable of providing a home for a rich diversity of life, our work is to ensure all in our communities grow into people of compassion and wisdom with a deep spiritual understanding of how to support the needs of others.

SCHOOL VISION

Click or tap here to enter text.

Table of Contents

LIST OF ANNEXES

1 Aims and scope

Information and communications technology (ICT) is an integral part of the way our school operates. It is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online

- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors, visitors, and anyone who has access to our IT and communication systems.

Misuse of IT and communications systems can damage our school and our reputation. Breaches of this policy may be dealt with under our Staff Professionalism and Code of Conduct and Disciplinary Policy (staff) and Behaviour Policy (pupils).

2 Legislation and guidance

This policy refers to, complies with, or otherwise has regard to, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) 2020
- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2025
- Searching, screening and confiscation: advice for schools 2022
- DfE cyber security standard (updated 2024)
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- Meeting digital and technology standards in schools and colleges
- Online Safety Act 2023
- Minimum requirements for cyber security cover of the Risk Protection Arrangement, which all schools of the Trust buy in to.

3 Definitions and acronyms

- **Authorised personnel**: employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **ICT facilities**: all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service

- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs
- **NCSC**: National Cyber Security Centre
- **Personal use**: any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Users**: anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors

See Annex II for a glossary of cyber security terminology.

4 Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see Section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Using the school's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the internet and network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation

- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Any uses categorised as unacceptable the school's "Mobile phone and smart technology policy" and "AI policy", "Behaviour Policy" and "Professionalism and code of Conduct".

This is not an exhaustive list. The school reserves the right to amend this list at any time. The [headteacher or any other relevant member of staff] will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion. Permission can only be granted in writing (e.g. by email).

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's Behaviour Policy / Staff Professionalism Policy and Code of Conduct. The Headteacher may put specific sanctions in place for unacceptable ICT use (e.g. revoking permissions to use the school's systems). Annex I provides an overview of specific sanctions for the unacceptable use of ICT in this school (if relevant) and links to the school's Behaviour Policy / Staff Professionalism Policy and Code of Conduct and Mobile Phone and Smart Technology Policy.

5 Staff (including governors, volunteers and contractors)

5.1 Access to school ICT facilities and materials

The school's school business manager (SBM), supported by the school's bought-in IT services provider, manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the SBM.

Detailed information on how requests to access files/facilities are processed in this school can be found in Annex I.

5.1.1 Use of school-supplied equipment

School-issued devices (including laptops, tablets and other digital devices) are provided to staff for the purpose of supporting teaching, learning and the efficient running of the school. All school-supplied equipment remains the property of the school and staff must return the equipment at the end of employment, or when it is no longer required. Staff must:

- Use equipment and devices primarily for school purposes and in line with the school's policies on safeguarding, data protection and confidentiality
- Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations
- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from school. E.g. when travelling on public transport, be aware that other passengers may be able to read any documents displayed on the screen of your device
- Lock devices with a password when unattended. The passwords must follow the guidance in Section 8.1.
- Complete NCSC cyber security training annually
- Update software, operating systems and applications when prompted, or as directed by IT support
- Connect to the school network using approved and secure methods.
- When connecting to wi-fi networks outside of the school, staff must ensure connections are secure and avoid transmitting sensitive data over public or unsecured networks
- Report any loss, theft, damage or compromise of a school device promptly to SBM and designated safeguarding lead (if relevant).

5.1.2 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only. Staff must make sure multi-factor authentication is enabled on their email account(s).

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to subject access requests from individuals under the UK GDPR and the Data Protection Act 2018 in the same way as paper documents. In that light staff are encouraged to not use full names in email communication and to be mindful that emails containing names of individuals can be disclosed to

them or people with parental responsibility. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted using a strong, state-of-the-art encryption standard so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the DPO immediately and follow the school's data breach procedure as laid out in the school's Data Protection Policy.

Staff must not give their personal phone number(s) to parents/carers or pupils. In circumstances where staff are provided with phones, these staff must use the phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in Section 4 and comply with the school's Mobile Phone and Smart Technology Policy.

The school can record incoming and outgoing phone conversations.

If you record calls or video conferences as standard, callers / participants must be made aware that the conversation is being recorded and the reasons for doing so (For instance: "All calls to the school office are recorded to aid administrators" or "Calls are recorded for use in staff training"). Your school's phone system and meeting software has an automated option you can use/adapt.

All non-standard recordings of phone conversations must be pre-approved by the Headteacher and consent obtained from all parties involved. This may be appropriate when:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

5.1.3 Professional standards in email communication

Email is a formal record of school communication and must reflect the school's professional standards at all times. The following applies to all staff using school email accounts.

Tone and content

All emails sent on behalf of the school must be:

- Written in a professional, clear and respectful tone, regardless of the circumstances or the nature of any dispute or complaint
- Factually accurate: staff must not make statements in email that they cannot evidence or would not be comfortable seeing disclosed in legal proceedings or a subject access request
- Free from discriminatory, offensive or inappropriate language
- Proofread before sending, particularly when communicating with parents, carers, external agencies or governors

Staff should never send an email when angry or upset. If a situation is emotionally charged, staff should draft their response and seek review from a line manager or the headteacher before sending.

Email signatures

All staff must use a consistent, professional email signature on all external correspondence. The signature must include the staff member's full name, job title, school name and the school's main contact details, in line with the Trust's and school's brand guidelines. Personal quotes, images or non-Trust branding must not be included in professional email signatures.

Group emails and mailing lists

When sending an email to a group of parents, carers or other individuals who do not know one another:

- Recipients must always be placed in the "blind copy" (Bcc) field, never in the To or Cc fields, to prevent personal email addresses being shared without consent
- Staff must double-check recipient lists before sending, particularly when using distribution groups or importing contacts from Arbor
- If an email is sent in error to the wrong recipient, or with recipients visible in the To/Cc field when they should have been Bcc'd, this must be reported immediately to the school business manager as a potential data breach, in line with Section 20 of this policy

Reply All and forwarding

Staff must use Reply All with care and only when a response is genuinely needed by all recipients. Emails containing personal data, confidential information or safeguarding content must never be forwarded to unauthorised recipients. Before forwarding any email chain, staff must review the full thread to ensure it does not contain information that should not be shared with the new recipient.

Handling unexpected or suspicious emails

Staff should treat unexpected emails from known contacts with the same caution as emails from unknown senders, particularly where the email asks the recipient to click a link, fill in a form, open an attachment, make a payment or provide login credentials. A trusted colleague's email account may have been compromised and used to send malicious content. If in doubt, verify the request by telephone before acting, and report the email to the School Business Manager or directly to the school's IT service provider. See also Section 9 and the glossary entry for Phishing.

Email retention and deletion

Emails must be retained or deleted in line with the school's records retention schedule and data protection policy. Staff must not use their school email inbox as a long-term filing system. Emails containing personal data should be deleted once they are no longer needed for the purpose for which they were sent, in line with the data minimisation principle under UK GDPR.

Communication with parents and carers about sensitive matters

Email is not always the appropriate channel for sensitive or complex communications with parents and carers, including matters relating to safeguarding, exclusions, SEN, attendance or complaints. In these cases, staff should consider whether a telephone call or face-to-face meeting is more appropriate and should seek guidance from their line manager or the headteacher before communicating by email on such matters. Where sensitive matters are discussed by email, the guidance on encryption in Section 8.8 applies.

AI use in the generation of emails

Emails drafted or substantially generated by AI tools must be reviewed carefully before sending to ensure they are accurate, appropriately personalised and reflect the professional standards above. An AI-generated email sent to a parent about a sensitive matter without sufficient human review is both a reputational and a safeguarding risk. See the school's AI policy for more guidance on the use of AI in schools (see link in Annex I)

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The headteacher may withdraw or restrict this permission at any time and at their discretion.

Occasional personal use is permitted provided that such use:

- Does not take place during school hours
- Does not constitute 'unacceptable use', as defined in Section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see Section 5.7). Where breaches of this policy are found, disciplinary action may be taken.

Staff are only permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Mobile Phone and Smart Technology policy and the Staff Professionalism Policy and Code of Conduct.

Staff may not store any school-related data on personal devices, on cloud storage or on personal removable storage devices.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, advertently or inadvertently putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media and use of email contained in the Staff Professionalism Policy and Code of Conduct (see Section 5.3.1) to protect themselves online and avoid compromising their professional integrity.

5.3.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

Staff is to follow the school guidelines regarding the appropriate security settings for social media accounts as laid out in the Staff Professionalism Policy and Code of Conduct.

5.3 Remote access

The Trust discourages the use of remote access facilities for staff. If the school still has this facility (usually in the context of a legacy locally hosted solution), staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as the SBM, on the advice of the school's IT support service, may require against importing viruses or compromising system security.

The school's ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with the school's data protection policy.

Add a link to the school's data protection policy can be found in Annex I.

5.4 School social media accounts

The school official social media accounts, and the name of the staff member who manages them, under the oversight of the headteacher, are listed in Annex I.

Only authorised staff may post to, or manage, the school's official social media accounts. Staff who have not been explicitly authorised to do so must not access, or attempt to access, these accounts.

Guidance on what may and must not be posted on school social media accounts can be found in Annex III

5.5 Use of Personal Messaging Applications (including WhatsApp)

The school recognises that personal messaging applications such as WhatsApp are widely used and that staff may find them convenient for quick communication. However, their use carries significant risks in a school context, including lack of an auditable record, data protection concerns, and the potential to create informal communication channels that undermine professional standards and team cohesion.

5.5.1 Staff-to-parent/carer communication

Staff must not use personal messaging applications to communicate with parents or carers about school matters. All communication with parents and carers must take place through the school's official channels, such as Arbor and the school email system. This is both a data protection requirement and a safeguarding boundary.

5.5.2 Staff-to-staff communication

The school's preferred and primary channel for work-related communication between staff is school email and Microsoft Teams (and/or Google Chat for google schools]. Staff are discouraged from using personal messaging apps such as WhatsApp for work-related communication, as these fall outside the school's monitoring and audit systems, may exclude colleagues, and can create informal decision-making channels that are inconsistent with the school's professional standards.

Where staff use messaging apps informally for non-sensitive team communication (e.g. a staff social group), this must remain clearly separate from school business, must not include sensitive information about pupils, parents or colleagues, and must comply with Section 16 of the Staff Code of Conduct.

5.5.3 School trips and off-site activities

The school recognises that on overnight or extended off-site visits, staff may need a rapid communication channel that does not depend on school email infrastructure. In these circumstances, the use of a school-managed group chat, set up on a school-provided device or a dedicated account, not a personal WhatsApp account, is the preferred approach.

Where no school-managed alternative is available and a personal messaging app is used for operational communication during an off-site visit, the following conditions apply:

- Prior written approval must be obtained from the headteacher
- The group must include only staff members directly involved in the trip — not parents or pupils
- No personal data about pupils (including names, medical details or images) may be shared through the app
- The group must be closed and messages deleted at the end of the visit
- Any safeguarding concern arising during the trip must still be reported through official channels and recorded in writing

5.6 School website

The school website is the school's primary public-facing channel and the authoritative source of information for parents, carers, prospective families and the wider community. It also carries statutory publication requirements that must be met at all times.

See Annex I indicates the name of the person who manages the school website, under the oversight of the headteacher. Only authorised staff may publish, edit or remove content from the school website.

5.7 Monitoring and filtering of the school network and use of ICT facilities

To comply with Department for Education (DfE) guidance on meeting digital and technology standards, and to safeguard and promote the welfare of children and provide them with a safe environment to learn, the school:

- Produces monitoring reports of the use of its ICT facilities and network at least weekly
- Produces ad-hoc, Immediate reports when required due to high-risk incidents (safeguarding, malicious or technical nature)
- Documents its use of monitoring reports as part of its incident handling records, including a description of the actions taken and outcomes.
- Reviews its filtering and monitoring system at least once per academic year

The schools filtering and monitoring system covers, but is not limited to:

- Internet sites visited
- Searches made
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Content of email messages
- Any other electronic communications

Only authorised personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The details about the filtering and monitoring system used in this school can be found in Annex I.

The purpose of the monitoring is, amongst others, to:

- Comply with DfE filtering and monitoring requirements
- Keep staff and children safe
- Find lost messages or retrieve messages lost due to computer failure
- Help in the investigation of alleged wrongdoing
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises

- Prevent or detect crime
- Comply with a subject access request, Freedom of Information request, or any other legal obligation

6 Pupils

6.1 Access to ICT facilities

An overview of the ICT facilities available to pupils at this school is in Annex I.

6.2 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with our Behaviour Policy, if a pupil engages in any of the following, at any time, whether or not they are on school premises or using school ICT equipment or on the school network:

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Any use prohibited in the school's AI policy

Any specific sanctions related to these infringements applied in this school can be are listed in Annex I.

7 Parents / Carers

7.1 Access to ICT facilities and materials

Parents/carers do not have access to the school's ICT facilities as a matter of course.

However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use the school's facilities at the headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school whether by phone, email, text, messaging services and through social media channels. They are expected to:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, in line with the school's complaints procedure. The link to the school's Complaints Policy can be found in Annex I.

Parents / carers may not:

- Use private groups, the school's social media pages, or personal social media to complain about or criticise members of staff. The school understands it will not always get it right and invites parents to follow its Complaints Policy to ensure that their concerns are dealt with in the most effective and constructive way possible.
- Under any circumstance use private groups, the school's social media pages, or personal social media to complain about, or try to resolve, a school-related behaviour issue involving other pupils. The class teacher or other appropriate member of staff should be contacted to report any behaviour issues or incidents involving another pupil.
- Upload or share photos or videos on social media of any child other than their own, unless it they have the explicit permission of the other children's parents/carers to do so.

7.3 Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

8 Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cybercrime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should always follow the safe practices for ICT use contained in this policy. The school adheres to the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

The school's Management Information System (MIS), Arbor, is the authoritative record for staff and pupil data, and its accuracy directly underpins the integrity of access controls across all school ICT systems. All staff with responsibility for maintaining MIS records share a duty to keep those records current.

8.1 Passwords and passkeys

All users are responsible for the security of their passwords and accounts and for setting permissions for the accounts and files they control. Passwords must be kept confidential (e.g. not written on a post-it note stuck to one's computer or written in a booklet that is not locked away at all times).

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

The NCSC actively recommends the use of passkeys over passwords wherever available. In line with the DfE Digital and Technology standards (2024) and NCSC guidelines, passwords must:

- be unique credentials per user — no shared logins
- follow NCSC guidelines, i.e. be either machine-generated passwords or a three random words system
- Not be shared with others
- Must be changed regularly
- Not be reused across multiple accounts

Passwords must be changed immediately if they are compromised or suspected of compromise, or when directed to do so by the SBM or IT support. Routine periodic password changes are not required.

Devices will be locked after more than 10 attempts in 5 minutes or after 10 failed attempts.

Staff may use reputed password managers to help them store their passwords securely.

Staff responsible for generating passwords for pupils will keep a copy of these encrypted and in a secure location, in case pupils lose or forget their passwords.

Network devices and servers require a minimum 6-character PIN/password unique to that device.

8.1.1 Multi-Factor Authentication (MFA)

MFA is mandatory for:

- All senior leaders and staff handling confidential, financial, personal or sensitive personal data
- All cloud-based applications accessed by staff working away from school
- All remote access to the network

The use of SMS-based second-factor authentication is discouraged in favour of the use of authenticators or Passkeys.

8.1.2 Passkeys

Recent NCSC guidance (April 2026) has advised that passkeys are at least as secure, and often more secure, than all forms of traditional MFA at every stage of the credential lifecycle.

8.1.3 Password managers

All staff are advised to use a password manager (tied to the school's existing infrastructure, such as Microsoft 365 or Google password management features) or the stand-alone password manager approved by the SBM / IT support team, to store their passwords securely. In line with NCSC guidance, the password manager used must store credentials in encrypted form and support unique passwords per account.

8.2 USB /removable storage

The use of USB and other removable storage devices are prohibited. In the exceptional circumstances that access would be required, this should be done under the guidance of the IT support service and scanned for malware before access.

8.3 Backups

The school buys into the DfE's Risk Protection Arrangement (RPA), which requires backups to be part of the business continuity plan. See Section 9.3 for further details.

8.4 Account lifecycle management

The headteacher ensures that a formal process is in place in the school for managing user accounts at every stage of employment or enrolment, aligned with the DfE's cyber security standards.

The process should ensure that:

- New starters (joiners): Accounts will be created and access rights assigned in advance of a new staff member's start date, based on their role as recorded in the MIS. No account should be created without prior authorisation from Headteacher. Staff may not begin using school ICT systems until their identity has been verified.
- Changes of role (movers): Where a member of staff changes role, their access rights must be reviewed and updated to reflect their new responsibilities. The previous role's access permissions must be revoked at the point of transition, not retrospectively. Any changes to access levels must be approved by headteacher before being actioned by the School Business Manager or the school's IT support service.
- Leavers: When a member of staff leaves, their account must be disabled on or before their last working day, without exception. All access to school systems, email, cloud services and remote access must be revoked at the same time. The school's IT support service must be notified of a leaver's last working date by the school business manager as soon as it is confirmed and no later than 5 working days before that date. The staff's record on the school's MIS (Arbor) must be updated on the same day.
- Termly access reviews: The SBM must instruct the school's IT support service to conduct a review of all active user accounts and their permissions at least once per term. The purpose of this review is to identify any accounts that are no longer needed, any permissions that have drifted beyond what a user's role requires, and any discrepancies between the MIS and active system accounts. The outcome of each review will be reported to headteacher
- Privileged accounts: Administrative or global accounts must not be used for routine day-to-day tasks. Staff with administrative access must use a separate, unprivileged account for general work, reserving their admin credentials solely for tasks that require elevated permissions.

8.5 Software updates, firewalls and anti-virus software

Automatic software updates, security updates and anti-virus products will be enabled on all school ICT devices that support this functionality.

Users should not delete, destroy or modify existing systems, programs, information or data. Users must not download or install software from external sources without authorisation from the school's IT support.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

The school has anti-virus software in place that scans all incoming files for viruses before they are downloaded.

Any personal devices using the school's network must all be configured in line with the requirements listed above.

8.6 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy. Annex I contains a link to the school's data protection policy.

8.7 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices, determined by their role.

Access rights are managed by the school's IT support under the instruction of the SBM, and are, wherever possible, provisioned automatically through integration with Arbor, the school's Management Information System (MIS). It is therefore essential that the MIS is kept accurate and up to date at all times, as changes to staff roles, employment status or pupil records will directly affect system access permissions.

Staff responsible for maintaining the Arbor, including the SBM and the administration team, must notify the school's IT support service promptly of any changes that affect access rights, including new starters, changes of role, and leavers, and must ensure the MIS record is updated at the same time.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the SBM immediately.

Users should always log out of systems and lock their equipment when not in use. Equipment and systems should always be logged out of and shut down completely at the end of each working day. This will also ensure that any critical software updates are completed.

8.8 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices to access school data, work remotely if they have been specifically authorised to do so by the headteacher. Authorisation can only be granted if the device has appropriate levels of security and encryption, as defined by the school IT support provider.

USB drives may not be used (see above) and personal data may not be downloaded onto personal devices.

9 Protection from cyber attacks

The school recognises that cyber-attacks pose a significant and growing risk to school operations, data security and safeguarding. This section sets out the school's approach to cyber resilience, in line with the DfE's cyber security standards and the conditions of the DfE Risk Protection Arrangement (RPA).

9.1 Governance and leadership

The school will:

- Appoint a digital lead from the senior leadership team. The name of the digital lead for the school is listed in Annex I. The digital lead holds overall responsibility for cyber security oversight, risk assessment and compliance with the DfE's digital and technology standards
- Ensure the Local Academy Committee receives an annual update on the school's cyber security posture, including the outcome of the annual cyber risk assessment and any significant incidents
- Ensure cyber security is given appropriate time, budget and resources, reviewed as part of the annual budget-setting process
- Conduct a cyber risk assessment at least annually, and revisit it every term or following any significant cyber event, led by the digital lead in conjunction with the school's IT support.

9.2 Staff Training

The school will provide annual cyber security training for all staff, governors and volunteers with access to school ICT systems. This training will be evidenced and recorded. It is a condition of the school's RPA cyber cover.

Training will cover, as a minimum:

- How to recognise phishing emails, including how to check sender addresses and identify suspicious links
- How to respond to requests for bank details, personal information or login credentials — and how to verify such requests through an alternative channel
- Password security and the use of the school's approved password manager
- Multi-factor authentication — what it is and how to use it
- The physical security of devices (e.g. not leaving a laptop unlocked and unattended, not using unsecured public Wi-Fi)
- The risks of removable storage media such as USB drives
- How and when to report a suspected cyber incident or attack
- How and when to report a data breach
- Social engineering tactics and how to avoid them
- Data protection responsibilities, with more frequent training for staff exposed to higher-risk data

New starters who join outside of the school's annual training window must complete this training as part of their induction, before being granted full access to school ICT systems.

9.3 Backups

Robust and tested backups are both a DfE requirement and a condition of the school's RPA cyber cover.

- The school follows the 3-2-1 backup rule:
- At least 3 copies of all critical data are maintained
- Stored on at least 2 separate devices or media
- With at least 1 copy stored off-site or in a secure, isolated cloud environment that is not directly connected to the school's main network

Critical data will be backed up at least daily, either automatically or as a managed process overseen by the SBM and executed by the IT service provider.

Backups will be tested at least termly to confirm that data can be successfully restored. The outcome of each test will be recorded and reported to the digital lead. A failed backup test must be escalated to the headteacher immediately.

In the event of a ransomware attack, the school will not pay any ransom demand, as this does not guarantee recovery of data and may expose the school to further risk. Recovery will be pursued through backup restoration and, where necessary, with support from the NCSC and the school's RPA provider.

9.4 Incident Response Plan

The school maintains a written cyber incident response plan, reviewed and tested at least annually. This is a condition of the school's RPA cyber cover.

The plan covers, as a minimum:

- Who is responsible for managing a cyber incident, which in this school is the digital lead (see Annex I)
- Which other staff members are involved: the headteacher, the SBM, the school's IT service provider and data protection officer (see Annex I for details).
- How the school will communicate internally and externally if normal communications systems are unavailable
- When and how to notify the ICO of a data breach (within 72 hours where required under UK GDPR)
- When and how to report the incident to Action Fraud and the NCSC
- When and how to notify the RPA of a cyber insurance claim
- How evidence will be preserved for investigation purposes
- A process for post-incident review and lessons learned

The incident response plan will be tested at least annually using the NCSC's Exercise in a Box tool and reviewed after any significant cyber event. The digital lead is responsible for ensuring the plan remains current.

9.5 Registration with Police CyberAlarm

The school is registered with Police CyberAlarm, as required under the RPA cyber cover conditions. The SBM, with the support of the school's IT service provider, is responsible for maintaining this registration and ensuring the monitoring tool remains active. The School Business Manager holds the CyberAlarm account credentials for the school.

9.6 Technical Controls

The school will maintain the following technical controls, in line with the DfE's cyber security standards:

- All necessary firewalls are in place, switched on, and cover all areas of the network
- Anti-malware software is installed on all devices and kept up to date
- Endpoint detection and response (EDR) systems are in place where appropriate
- Software security updates notified by the DfE must be applied within 5 working days of notification; all other critical updates are applied promptly
- USB and removable storage devices are disabled by default; any exceptions require prior authorisation from the [ICT manager/network manager], and all removable media must be scanned for malware before use
- If relevant, staff dial into the school network remotely using a virtual private network (VPN)
- The school's supply chain is kept under review; key suppliers are asked to demonstrate their cyber security credentials, including whether they hold Cyber Essentials or equivalent certification

9.7 Monitoring and Review

The school will:

- Conduct a third-party cyber security audit (such as 360 Degree Safe or equivalent) at least annually to objectively assess the effectiveness of controls
- Ensure the incident response plan is reviewed and tested at the frequency set out in Section 9.4
- Ensure the annual cyber risk assessment is reviewed termly and after any significant event
- Report the outcomes of audits, risk assessments and incident response tests to the governing board annually

10 Internet Access

The school's wireless internet connection is secure.

For further details about the school's WIFI arrangements can be found in Annex I.

10.1 Pupils

Pupils are permitted to access the internet through school-managed devices only, under staff supervision and in accordance with this policy and the school's behaviour policy.

In line with DfE guidance (January 2026), the school operates as a mobile phone-free environment by default. Pupils are not permitted to use personal mobile phones, smart watches or other personal smart technology during the school day, including during lessons, between lessons, at break time and at lunch time. This prohibition extends to connecting any personal device to the school's Wi-Fi network.

The school's approach to mobile phones and smart technology is set out in full in the school's Mobile Phone and Smart Technology Policy, which should be read alongside this policy. Any exceptions to the default prohibition — for example for pupils with a medical need — are managed in accordance with that policy and in compliance with the Equality Act 2010.

Where pupils use school-managed devices to access the internet, the school filtering, supervision and reporting arrangements are described in Annex I.

10.2 Staff

Staff may access the school's Wi-Fi network using school-managed devices for work purposes. Staff are expected to model the school's mobile phone-free culture and in line with the school's Mobile Phone and Smart Technology Policy, staff must keep personal devices and locked in a locker/drawer and at a mininum switched off or set to silent during lesson times. Personal use of the school's Wi-Fi network should the requirements laid out in the Mobile Phone and Smart Technology Policy.

10.3 Parents/carers and visitors

Parents, carers and visitors will not be permitted to use the school's Wi-Fi network unless specific authorisation is granted by the headteacher. Authorisation will only be granted where:

- A parent or carer is working with the school in an official capacity (e.g. as a volunteer or member of the PTA)
- A visitor needs to access the school's Wi-Fi to fulfil the purpose of their visit (e.g. to access materials stored on a personal device as part of a presentation)

Staff must not give the Wi-Fi password to any unauthorised person.

10.4 Compliance commitment

Pupils are expected to comply with these provisions as part of the school's Behaviour Policy and frequently referred to in a class context.

Expectations related to parents are incorporated in each pupil's home-school agreement. The wording regarding acceptable ICT use in this agreement follows the template in

Staff expectations in this area are part of the school's Staff Professionalism Policy and Code of Conduct. staff agreement. All staff are expected to acknowledge that they have read the code of conduct in either the school's MIS or Smartlog (see Annex I for the provisions in this school).

Visitors sign a short declaration, along the lines of "I agree to use the school's ICT facilities in accordance with the school's acceptable use policy, a copy of which is available on request" on the school's visitor sign-in system.

11 Monitoring and review

The headteacher, SBM and digital lead monitor the implementation of this policy, including notifying the Trust central team of any updates that would be required to reflect the needs and circumstances of the school.

This policy will be reviewed and approved every 2 years by the Trust Board of Directors.

12 Related policies

Adapt this list as required.

This policy should be read alongside the school's policies on:

- Artificial Intelligence
- Safeguarding and child protection
- Behaviour
- Staff Professionalism and Code of Conduct
- Online safety
- Data protection
- Mobile phone and Smart Technology

[Insert school name and logo]

Annex I - School-specific information related to this policy

Key roles

- The headteacher of the school is: [name, contact details]
- The SBM of the school is: [name, contact details]
- The digital lead for the school is: [name, role, contact details (can give generic school contact details)]
- The IT service provider for the school is: [name company]. All contact with the school's IT service provider should be through the School Business Manager.
- The school's Data Protection Officer is [name], Grow Education Partners.

How requests to access files/facilities in this school:

[state if requests should go to SBM / by email/does SBM issue ticket to external IT support or do it themselves – if individuals need to request it directly, provide info needed of the external IT support provider (email or link to their ticketing service – does it work if they don't have login details? If not, how / where do they request that?]

The school's WIFI arrangements are as follows:

[State here if separated access for staff/visitors/pupils, relevant technical details, DO NOT provide your WIFI SSID/PW here! As per the policy, access is not routinely granted to visitors]. Details on filtering and monitoring systems in place.

School Website

Link to the school website: [school website link]

School website manager (under the supervision of the Headteacher): [name]

The school has the following official social media accounts. The name of the staff member who manages them is indicated in brackets.

- Instagram: [Account identifier], [name of person managing] (if relevant)
- Facebook: [Account identifier], [name of person managing] (if relevant)
- LinkedIn: [Account identifier], [name of person managing] (if relevant)
- [Other]

An overview of the ICT facilities available to pupils at this school :

[Explain which ICT facilities are available to pupils, when and under what circumstances, for example computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff. Where pupils use school-managed devices to access the internet, describe any additional student-specific school filtering systems in place, and specify supervision and reporting arrangements in the school.

[Insert school name and logo]

Email addresses and passwords are provided to pupils, for educational purposes only. Pupils must not share their passwords with others, or use their email account to share or download files, including software from the Internet or inappropriate content, without the permission of [insert member of staff]

Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff

Pupils will be provided with an account linked to the school's virtual learning environment, which they can access from any device by using the following URL [insert web address]

school's WiFi arrangements. For instance:

Whether you use filtering

Whether you have separate connections for staff/pupils/parents or carers/the public

and how to report inappropriate sites that the filter may not have identified, or appropriate sites that have been filtered in error

[Describe filtering arrangements]

[Describe supervision arrangements]

[Describe how pupils can report inappropriate content or sites filtered in error]

Specific sanctions for the unacceptable use of ICT in this school: [if relevant, else delete]:

___

___

Location of the related school policies [or link]:

- AI Policy: [location]
- Behaviour Policy: [location]
- Complaints Policy: [location]
- Staff Disciplinary Policy [location – internal]
- Staff Professionalism Policy and Code of Conduct: [location - internal]
- Mobile Phone and Smart Technology Policy: [location]
- Data Protection Policy: [location]

Annex II - Definitions

TERM	DEFINITION
3-2-1 Backup Rule	The 3-2-1 rule is the internationally recognised standard for safe data backups. It means maintaining at least 3 copies of important data, stored on at least 2 different types of media or device, with at least 1 copy stored off-site or in an isolated cloud environment that is not directly connected to the school's main network. Following this rule means that if the school suffers a ransomware attack, hardware failure or fire, a clean copy of the data can still be recovered. The 3-2-1 rule is a condition of the DfE's Risk Protection Arrangement (RPA) cyber cover.
Adversary-in-the-Middle (AitM) Attack	An adversary-in-the-middle attack is a sophisticated form of phishing in which a criminal secretly positions themselves between a user and a legitimate website or service, intercepting login credentials and authentication codes in real time. This means that even if a user has multi-factor authentication enabled, an AitM attack can capture and reuse the session before the user realises anything is wrong. This is why the NCSC now recommends passkeys and hardware security keys above SMS-based MFA, as these are resistant to AitM attacks.
Antivirus software	Software designed to detect, stop and remove viruses and other kinds of malicious software.
Breach	When your data, computer systems or networks are accessed or affected without authorisation
Business Email Compromise (BEC)	Business email compromise is a type of fraud in which a criminal impersonates a trusted person, such as the headteacher, school business manager or a supplier, by sending emails that appear to come from a legitimate address. The aim is typically to trick staff into making an unauthorised payment, changing bank account details, or sharing sensitive information. BEC attacks are one of the most common and financially damaging cyber threats facing schools. Staff should always verify requests to change payment details or authorise transactions through a separate, known channel (e.g. a phone call to a known number) before acting.
Cloud	An on-demand, massively scalable service, hosted on a shared infrastructure where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.

TERM	DEFINITION
Cyber Essentials	Cyber Essentials is a UK government-backed certification scheme, overseen by the NCSC, that certifies organisations as having met a baseline standard of cyber security. There are two levels: Cyber Essentials (self-assessed) and Cyber Essentials Plus (independently verified). Schools are encouraged to work towards Cyber Essentials certification themselves, and the DfE recommends that schools check whether their key suppliers hold this certification as part of managing supply chain risk.
Cyber incident	Any event that threatens the confidentiality, integrity, or availability of data within your computer network, or where the security of your system or service has otherwise been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from unauthorised theft or damage.
Deepfake / Synthetic Media	A deepfake is a video, audio recording or image that has been artificially created or manipulated using artificial intelligence to make it appear that a real person said or did something they did not. Deepfakes are relevant to schools in two ways: as a safeguarding risk (pupils creating or sharing manipulated images of other pupils or staff), and as a social engineering risk (criminals using AI-generated voice or video to impersonate trusted individuals). KCSIE 2025 identifies synthetic media as an emerging online harm.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Endpoint Detection and Response (EDR)	EDR is a type of security software installed on individual devices (endpoints) such as laptops, computers and tablets. Unlike traditional anti-virus software, which looks for known threats, EDR continuously monitors device behaviour in real time and can detect, contain and respond to suspicious activity, including previously unknown attacks. The DfE recommends EDR as part of a school's cyber security controls.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Generative AI	Generative AI refers to artificial intelligence systems that can create new content, including text, images, audio, video and computer code, in response to a user's instructions (known as a "prompt"). Tools such as ChatGPT, Microsoft Copilot and Google Gemini are examples of generative AI. The use of generative AI by staff and pupils raises questions about data protection, academic integrity, safeguarding and copyright that are addressed in the school's separate AI policy, to which this policy should be read as complementary.
Hacker	Someone who uses their technology skills to gain unauthorised access to computers, systems and networks.
Malware	Malicious software. Any kind of software that can damage computer systems, networks or devices, which includes viruses, trojans or any code or content that is harmful.

TERM	DEFINITION
Multi-Factor Authentication (MFA)	Security measure that requires a user to prove their identity in two or more ways before being granted access to an account or system. These factors typically combine something the user knows (such as a password or PIN), something the user has (such as a phone or hardware security key), and something the user is (such as a fingerprint or face scan). MFA is a mandatory requirement under the DfE's cyber security standards for all staff accounts that have access to personal, confidential or financial data, and for all remote access to school systems. Not all forms of MFA offer the same level of protection. In order of increasing security, the most common methods are: SMS one-time codes (vulnerable to SIM-swap fraud and adversary-in-the-middle attacks; Authenticator apps (significantly more secure, recommended minimum standard for school staff); Passkeys and hardware security keys (most secure form of MFA, resistant to phishing and adversary-in-the-middle attacks; recommended by the NCSC as the preferred approach where supported.
Passkey	A passkey is a modern, more secure alternative to a password. Instead of typing a password, a user proves their identity using something they already have, such as their phone or laptop, combined with a fingerprint, face scan or PIN. Passkeys cannot be stolen through phishing because they never leave the user's device and are never typed or transmitted. The NCSC now recommends passkeys as the preferred form of authentication where they are supported.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses with the end aim of fixing them.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Form of cyber-attack in which a criminal impersonates a trusted person or organisation, such as a bank, government department, software provider or colleague, to trick the recipient into revealing sensitive information (such as passwords or financial details), clicking a malicious link, opening an infected attachment, or transferring money. Phishing most commonly arrives by email, but has evolved into several related variants that staff should be equally alert to (see definitions elsewhere in this list): Spear phishing, whaling, smishing, vishing. Phishing emails and messages often create a false sense of urgency, warning the recipient that an account will be suspended, a payment has failed, or that immediate action is required. Common warning signs include unexpected requests, mismatched or slightly altered sender addresses, generic greetings, and links that do not match the organisation they claim to be from.

TERM	DEFINITION
	Staff should never click a link or open an attachment in an unexpected message without first verifying its legitimacy through an independent channel. Any suspected phishing attempt should be reported immediately to the School Business Manager or directly to the school's IT Support Provider.
Police CyberAlarm	Police CyberAlarm is a free tool provided by UK policing that monitors the internet traffic entering and leaving an organisation's network, and reports on suspicious activity. It acts as a "CCTV camera" for cyber threats, helping schools understand the volume and type of attacks being directed at them. Registration with Police CyberAlarm is one of the four mandatory conditions for schools to maintain cyber cover under the DfE's Risk Protection Arrangement (RPA).
Ransomweare	Malicious software that stops you from using your data or systems, usually by encrypting your files, until you make a payment (a ransom) for decryption.
Smishing	Smishing is a form of phishing carried out via SMS text message rather than email. A smishing message typically claims to be from a trusted organisation — such as a delivery company, bank or government body — and contains a link designed to steal login credentials or personal information, or to install malware on the recipient's device. Staff should treat unexpected text messages containing links with the same caution as suspicious emails.
Social engineering	Manipulating people into giving information or carrying out specific actions that's of use to an attacker.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Supply Chain Attack	A supply chain attack occurs when a cyber-criminal targets a school not by attacking the school directly, but by compromising a supplier, software provider or contractor that the school trusts and has connected to its systems. For example, if a school's MIS provider or cloud service were compromised, an attacker could use that trusted connection to access the school's data. Schools should ask key suppliers to demonstrate their cyber security credentials, such as Cyber Essentials certification.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.

TERM	DEFINITION
Vishing	Vishing (voice phishing) is a social engineering attack carried out over the telephone. A caller impersonates a trusted individual or organisation, such as a bank, IT support provider, or government department, to trick the recipient into revealing passwords, financial details or personal information, or into taking an action such as making a payment or installing software. Staff should be aware that callers claiming to be from IT support and asking for login credentials or remote access to devices should always be treated with suspicion and verified through an independent channel before any access is granted.
Whaling	A form, of spear phishing aimed specifically at senior leaders, such as headteachers or school business managers, often with the goal of authorising fraudulent payments (see also: Business Email Compromise)

[Insert school name and logo]

LDBS Academies Trust

Annex III - Posting to School Social Media Accounts

Authorised School Social Media Users

Only staff explicitly authorised by the Headteacher may post to, or manage, the school's official social media accounts. Staff who have not been explicitly authorised to do so must not access, or attempt to access, these accounts. All social media accounts should follow the Trust's and School's brand guidelines.

Purpose and Tone

The school's social media accounts exist to:

- Celebrate pupil achievements, school life and community events
- Share relevant information about the school with parents, carers and the wider community
- Promote the school's Christian ethos and values
- Engage positively with the local community and stakeholders
- All content posted on behalf of the school must reflect the school's professional standards and values, and should be written in a positive, inclusive and accessible tone. Posts must never be made when the author is angry, upset or under pressure — if in doubt, draft the post and return to it after a period of reflection, or seek approval from the headteacher before posting.

What May Be Posted

Staff authorised to manage school social media accounts may post:

- Photographs and videos of school events, trips and activities, provided that image consent has been obtained for all pupils featured in line with the school's data protection policy
- Celebration of pupil work and achievements, without identifying individual pupils by full name
- Information about upcoming events, term dates, closures and school news
- Links to resources, guidance or information relevant to the school community, provided these have been checked for accuracy and appropriateness
- Responses to comments or messages from parents and carers, provided these are factual, professional and do not disclose personal or confidential information

What Must Not Be Posted

The following must never be posted on the school's official social media accounts:

- Images or videos of pupils without verified consent in line with the school's image use policy and UK GDPR
- Full names of individual pupils, or any combination of information that could be used to identify a pupil (e.g. first name combined with year group and image)
- Personal data about any individual, including staff, pupils or parents/carers
- Any content that could be considered discriminatory, offensive, politically partisan or contentious
- Comments about, or responses to, complaints, disputes or legal matters — these must always be handled through the school's official complaints procedure and managed by the headteacher

- Content that has not been verified for accuracy — staff must not share news stories, statistics or guidance without checking the source
- Content that could bring the school, the Trust, or the profession into disrepute
- Promotional content for private businesses or personal interests, unless formally agreed with the headteacher
- Content about safeguarding incidents, exclusions, or any matter that is subject to investigation or legal proceedings

Platform-specific risks

- **Instagram and TikTok** have younger user bases and higher risks around image sharing and viral content. Posts involving pupils require particular care
- **Facebook parent groups operated by parents independently of the school** are outside the school's control, but staff should be aware that what they post on official accounts may be shared into those groups
- **X (formerly Twitter).** The Trust discourages the use of school X accounts as the platform has significantly reduced content moderation, relaxed verification standards and reinstated previously banned accounts, creating an environment in which schools have less control over the context in which their content appears, the nature of replies and interactions it attracts, and the values of the platform with which the school is publicly associated. Note also that X has a public-by-default setting: Should X be used, ensure the account privacy settings are reviewed regularly and consider whether a different platform (or at minimum a protected account) is more appropriate for a primary school audience.

Responding to Comments and Messages

Staff managing school accounts must monitor comments and direct messages regularly. The following applies:

- Positive, factual comments from parents and community members may be acknowledged with a like or a brief, professional response
- Questions or requests for information should be directed to the school office through official channels rather than answered in a public comment thread
- Negative, offensive or abusive comments must not be responded to in the heat of the moment. These should be screenshot, reported to the headteacher, and either hidden or deleted. A record should be kept in case of escalation.
- The school will not engage in public debates or disputes via social media. Any attempt to draw the school into a public disagreement should be referred to the headteacher immediately
- Direct messages from parents or carers about specific pupils or sensitive matters must not be responded to via social media — the sender should be directed to contact the school office

Images and Photography

Before any image or video featuring a pupil is posted to a school social media account, the authorised member of staff must confirm that:

- Written consent for online publication has been obtained from the pupil's parent or carer, in line with the school's image use policy

- The pupil is not subject to any court order, injunction or safeguarding arrangement that restricts publication of their image or location — if in doubt, check with the DSL before posting
- The image does not reveal the pupil's home address, travel route or any other information that could compromise their safety
- Any images generated using or enhanced by AI are clearly labelled as such, in line with emerging good practice on synthetic media

Account Security

School social media account credentials must:

- Be stored securely using the school's approved password manager, not in a personal account or on a personal device
- Never be shared with unauthorised staff, and must be changed immediately if a member of staff with access leaves the school or changes role
- Use multi-factor authentication where the platform supports it

The School Business Manager must hold a record of all school social media account credentials and be notified immediately if credentials are changed or if an account is believed to have been compromised.

Archiving and Records

A record of all posts made on behalf of the school should be retained in line with the school's records retention schedule. Where the school uses a social media management tool [e.g. Hootsuite, Buffer], posts should be archived automatically. Where posts are made directly to a platform, screenshots or exports should be saved periodically to the school's shared drive.

Annex IV – School Website

Only authorised staff may publish, edit or remove content from the school website. All website pages should abide by the Trust's and School's brand guidelines.

Statutory Content

The school is required by law to publish specific information on its website under the School Information (England) Regulations and related DfE guidance. The Headteacher is responsible for ensuring that all statutory content is present, accurate and up to date. A review of statutory content will be conducted at least termly, and always following any change to school leadership, policies, or DfE requirements.

Statutory content includes, but is not limited to: the school's vision and values, admissions arrangements, curriculum information, pupil premium strategy, SEND information report, accessibility plan, and all current school policies required for publication.

What May Be Published

Authorised staff may publish:

- Factual information about the school, its staff, curriculum, policies and procedures
- Celebration of school life, events and pupil achievements, subject to the image and data requirements (see below).
- Links to verified external resources relevant to pupils, parents and carers
- News and updates about the school, provided these are accurate, professionally written and approved by the headteacher before publication

What Must Not Be Published

The following must never be published on the school website:

- Images or videos of pupils without verified written consent in line with the school's image use policy and UK GDPR
- Full names of individual pupils, or any combination of information that could identify a pupil
- Personal data about any individual, including home addresses, contact details or medical information
- Content that has not been checked for accuracy, including links to external sites that have not been reviewed
- Content relating to complaints, disputes, ongoing investigations or legal proceedings
- Politically partisan, discriminatory or contentious content
- Content about any pupil who is subject to a court order, injunction or safeguarding arrangement that restricts publication of their image, identity or location — the DSL must be consulted before publishing content about any such pupil
- AI-generated images presented as real photographs without disclosure

Accessibility

- The school's website must comply with the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018, which require public sector websites to meet the WCAG 2.1 AA accessibility standard. This means that:

All images must have appropriate alternative text descriptions

- Documents published on the website (e.g. PDFs) must be in an accessible format wherever possible
- The school must publish and maintain an accessibility statement on the website
- Any accessibility issues identified must be logged and addressed promptly
- The School Business Manager is responsible for monitoring accessibility compliance and updating the accessibility statement at least annually.

Content Review and Removal

All website content must be reviewed at least annually to ensure it remains accurate, current and appropriate. Outdated content, including references to former staff, superseded policies, past events and expired information, must be removed promptly.

A content audit will be conducted at the start of each academic year, and a record of the audit kept by the School Business Manager.

Website Security

Website login credentials must be:

- Stored securely using the school's approved password manager
- Never shared with unauthorised individuals
- Changed immediately when a member of staff with access leaves the school or changes role

The website platform and any plugins or extensions must be kept up to date with security patches, in line with the school's software update requirements in this Policy. The School Business Manager must ensure that they are notified immediately by their website provider if the website is suspected of having been compromised.

Annex V - Template wording on Acceptable ICT use in the school's Home-School Agreement

ICT, INTERNET AND ONLINE SAFETY

The school will:

- Provide pupils with access to school ICT equipment and the internet for educational purposes, under appropriate supervision
- Put in place filtering and monitoring systems to help keep pupils safe online while using school systems
- Teach pupils about how to stay safe online, use technology responsibly, and recognise and report concerns, as part of our curriculum
- Communicate clearly with parents and carers about any online activity pupils are asked to complete at home, including the platforms or websites involved
- Take all reports of online bullying, inappropriate content or safeguarding concerns seriously and respond promptly in line with our policies
- Ensure that any images or videos of pupils are only published online with the written consent of parents or carers, and in line with our image use and data protection policies

As a parent or carer, I/we agree to:

- Support the school's approach to online safety and reinforce its expectations at home
- Not share images, videos or information about other pupils on social media or messaging apps, including in parent group chats, without the consent of those pupils' families
- Communicate with the school through official channels (such as [insert platform, e.g. Arbor, school email]) rather than through personal messaging apps or social media
- Contact the school promptly if I have any concerns about my child's online safety or about content my child has encountered, whether at school or at home
- Read and support the school's ICT and Internet Acceptable Use Policy, a copy of which is available on the school website here [insert link].

As a pupil, I agree to:

[Version A – for pupils in Y5 and 6]

- Use school computers, tablets and the internet only for learning, and only when a member of staff has said I can
- Keep my passwords private and never share them with friends
- Tell a trusted adult straight away if I see anything online that makes me feel worried, upset or uncomfortable — whether at school or at home
- Be kind and respectful to others online, just as I would be in person
- Not take photos or videos of other pupils or staff using any device without permission
- Follow the school's rules about mobile phones and smart technology

[Version B – for pupils up to and including Y4]

I will use computers and tablets for learning. I will keep my password secret. If something online worries me or makes me feel unsafe, I will tell my teacher or another adult I trust straight away.

[The home-school agreement contains a cross reference to this policy, with wording along the lines of:

Full details of the school's expectations for ICT and internet use are set out in our ICT and Internet Acceptable Use Policy, our Mobile Phone and Smart Technology Policy, and our Online Safety Policy, all of which are available on the school website. By signing this agreement, parents, carers and pupils confirm they have been made aware of these policies and agree to support them.]